

REMARKS

Claims 1-15 are pending.

The final Office Action mailed July 26, 2005 rejected claims 1, 3, 5, 8, 10, and 12-15 as obvious under 35 U.S.C. § 103(a) based on *Hypponen et al.* (U.S. 2003/0191957) in view of *Hodges et al.* (U.S. 6,035,423); claims 2, 4, 7, and 9 over *Hypponen et al.* and *Hodges et al.* further in view of *Almogly et al.* (U.S. 2002/0194489); and claims 6 and 11 over *Hypponen et al.* and *Hodges et al.* further in view of *Caccavale* (U.S. 2002/0129277).

The rejection of claims 1-15 is respectfully traversed because neither *Hypponen et al.* nor *Hodges et al.* teach or otherwise suggest the features of the claims. For example, independent claim 1 recites (emphasis added):

1. (Original) A network security system to be deployed between **a plurality of intranets belonging to respective organizations** and an internet backbone, comprising:
 - a scanning system **coupled to the intranets** for scanning incoming electronic mail for malicious code;
 - an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and
 - a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:
 - directing incoming electronic mail from the internet backbone to the scanning system.

Accordingly, claim 1 recites a “scanning system **coupled to the intranets** for scanning incoming electronic mail for malicious code” in a “network security system to be deployed between a plurality of **intranets belonging to respective organizations** and an internet backbone.” This feature is neither taught nor suggested in either *Hypponen et al.* or *Hodges et al.*

Hypponen et al. is directed to distributed computer virus detection and scanning (Title). Referring to FIG. 1 and the Abstract, *Hypponen et al.* describes a “method of detecting viruses in

a computer network 1 comprising intercepting data at at least one data transit node 4 of the network 1. The transit node 4 . . . transfers the identified data to a virus scanning server 7 over the network 1.” However, *Hypponen et al.* only shows one computer data network 1 in addition to the Internet 5 and has no disclosure of a “plurality of intranets,” much less a “scanning system coupled to the intranets.” Although the Office Action, p. 2, reads an “intranet” on the network 1 of *Hypponen et al.*, every feature of the claims, including the plural “intranets,” must be found in the applied references, and *Hypponen et al.* lacks the recited plural “intranets.”

In the “Response to Arguments” section, the Office Action (pp. 6-7) states:

However, Hypponen discloses the transit node is coupled to a network and the transit node can be coupled to an external network or the transit node may be an internal node of the network (Hypponen: [0012]). On the other hand, the network can comprise a plurality of nodes and some of the nodes may be network server of another intranets [*sic*]. Therefore, one with ordinary skill in the art would apply the method disclosed by Hypponen in any environment.

The Office Action here focuses on paragraph [0012] of *Hypponen et al.*, which states:

The transit node may be a gateway coupling the network to an external system or network, e.g. the Internet. Alternatively, the transit node may be an internal node of the network.

The next paragraph further clarifies the “transit node” (paragraph 13):

Preferably, the transit node is one of a database server, an electronic mail server, an Internet server, a proxy server, and a firewall.

Nowhere does *Hypponen et al.* suggest that any node of the network 3 of Figure 1 is a network server of “another intranet” as proposed by the Office Action, much less any nodes enabling a “network security system to be deployed between a plurality of **intranets belonging to respective organizations** and an internet backbone.” Thus, the Office Action merely engages in a wishful hindsight discussion of what the network “can comprise” and what some of the nodes “can be.” This reasoning by the Office Action contravenes 35 U.S.C. § 132, which requires the Director to “notify the applicant thereof, stating the reasons for such rejection.” This

section is violated if the rejection “is so uninformative that it prevents the applicant from recognizing and seeking to counter the grounds for rejection.” *Chester v. Miller*, 906 F.2d 1574, 15 USPQ2d 1333 (Fed. Cir. 1990). This policy is captured in the Manual of Patent Examining Procedure. For example, MPEP § 706 states that “[t]he goal of examination is to clearly articulate any rejection early in the prosecution process so that applicant has the opportunity to provide evidence of patentability and otherwise respond completely at the earliest opportunity.” Furthermore, MPEP § 706.02(j) indicates that: “[i]t is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to reply.”

To the extent the Office Action relies on “common knowledge” in its assertions, Applicants respectfully submit that the APA requires the Patent Office to articulate and place on the record the “common knowledge” used to negate patentability. *In re Zurko*, No. 96-1285 (Fed. Cir., Aug. 2, 2001). *In re Lee*, 277 F.3d 1338, 1344-45, 61 USPQ2d 1430, 1434-35 (Fed. Cir. 2002). Ordinarily, there must be some form of evidence in the record to support an assertion of common knowledge. See *Lee*, 277 F.3d at 1344-45, 61 USPQ2d at 1434-35 (Fed. Cir. 2002); *Zurko*, 258 F.3d at 1386, 59 USPQ2d at 1697 (holding that general conclusions concerning what is “basic knowledge” or “common sense” to one of ordinary skill in the art without specific factual findings and some concrete evidence in the record to support these findings will not support an obviousness rejection).

Hodges et al. too fails to disclose the plural “intranets” recited in the claims. Though the Office Action did not rely on *Hodges et al.* for this claim feature, it is evident from FIG. 10 of *Hodges et al.*, that there is only one corporate computer network **1006** on its side of the internet **1004**.

Independent claim 3 too is allowable over *Hypponen et al.* and *Hodges et al.* because neither reference shows “a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code.” As for independent claim 5, neither *Hypponen et al.* nor *Hodges et al.* show a “plurality of scanning systems coupled to the intranets for scanning incoming electronic mail for malicious code.”

Independent claim 8 and 10 recite: “downloading anti-virus code to clients coupled to the intranets.” As neither *Hypponen et al.* nor *Hodges et al.* show plural intranets, they do not render independent claims 8 and 10 obvious.

Dependent claims 2, 4, 6, 7, 9, and 11 are patentable for at least the same reasons as their independent claims and are individually patentable on their own merits. For example, none of the secondary references, *Almogly et al.* and *Caccavale*, disclose the “plurality of intranets belonging to respective organizations.”

As another example, *Almogly et al.* does not disclose the “decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications received via the internet backbone” as recited in claims 2 and 4. In fact, *Almogly et al.* does not even show a “decoy server” nor a server that masquerades as a legitimate server as recited in claim 2, but what it calls “decoy addresses.” Paragraph 153 (p. 7) of *Almogly et al.* states: “one or more decoy addresses are inserted into either or both address book 102 and folders 104.” *Almogly et al.*’s decoys are entities that are inserted into an address book; they are not servers.

In the “Response to Arguments” section, the Office Action (p. 7) states:

However, *Almogly* discloses a virus detection and containment system which include at least one computer configured with at least one decoy address, and a server operative to identify activity occurring at the computer, the activity involving the decoy address (*Almogly*: [008]). The computers are being used as decoys to detect viruses.

Again, the Office Action engages in wishful claim construction, completely ignoring “decoy server coupled to the intranets **for masquerading as a legitimate server** and logging activity on communications received via the internet backbone” as recited in claims 2 and 4. A “server operative to identify activity occurring at the computer,” as urged by the Office Action, does not obviate the features clearly recited by claims 2 and 4.

Dependent claim 7 recites “a plurality of decoy servers coupled to the intranets for masquerading as legitimate servers and logging activity on communications received via the internet backbone.” Since *Almogy et al.* does not even show one such decoy server, it clearly does not show a plurality of such decoy servers.

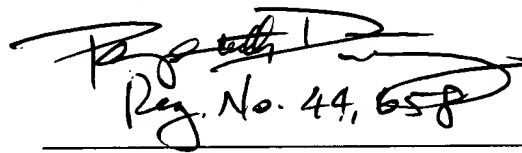
Moreover, dependent claim 9 recites: “simulating the decoy server as a legitimate server to the suspicious traffic.” *Almogy et al.*’s decoy addresses are not simulated as a legitimate server.

Dependent claims 12-15 are allowable for at least the same reasons as their respective independent claims, and are separately patentable on their own merits. Therefore, the rejections of all pending claims should be withdrawn.

Therefore, the present application overcomes the objections and rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at (703) 425-8501 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.



Reg. No. 44,658

9/26/05
Date

Margo Livesay, Ph.D.
Attorney/Agent for Applicant(s)
Reg. No. 41,946

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. (703) 425-8501
Fax. (703) 425-8518